OPSEC Countermeasures

Michael Chesbro
DES OPSEC Officer

Operations Security

Operations security (OPSEC)

As defined in DOD Directive (DODD) 5205.02, OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

(a) Identify those actions that can be observed by adversary intelligence systems.

(b) Determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

(c) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Operations Security

OPSEC protects critical information from adversary observation and collection in ways that traditional security programs cannot.

Simply put... OPSEC are those things that we do to prevent or limit the ability of an adversary to gather information about us!

What Information Should We Protect?

(Critical Information)

"Information about government personnel, officers, important personalities, and all matters related to them (residence, work place, times of leaving and returning, **and children**)."

– Al Qaeda Handbook

Criminals, con-artists, identity thieves, stalkers… all want to collect information about you and your family…

What Information Should We Protect?
(Critical Information)

- Military movements (deployment/redeployment dates, dates of field exercises, flight information etc.)… next Tuesday IS a specific date

- Any issues with the unit

- Anything concerning security

- Equipment issues (what, no flak vests?)

- Locations of units (it’s OK to say they’re in Afghanistan, but not to say that your spouse's battalion is at 14th and Ramadan in Tora Bora)

OPSEC Countermeasures

- Be careful what you post on social media sites (Facebook, MySpace, web-pages).
- Be careful what re (i.e. bumper sti

OPSEC Countermeasures

- Take a close look at all privacy settings. Set security options to allow visibility to “friends only.”
- Do not reveal sensitive information about yourself such as schedules and event locations.
- Ask, “What could the wrong person do with this information?” and “Could it compromise the safety of myself, my family or my unit?”
- Closely review photos before they go online. Make sure they do not give away sensitive information which could be dangerous if released.
- Make sure to talk to family about operations security and what can and cannot be posted.
- Videos can go viral quickly, make sure they don’t give away sensitive information.

OPSEC Countermeasures

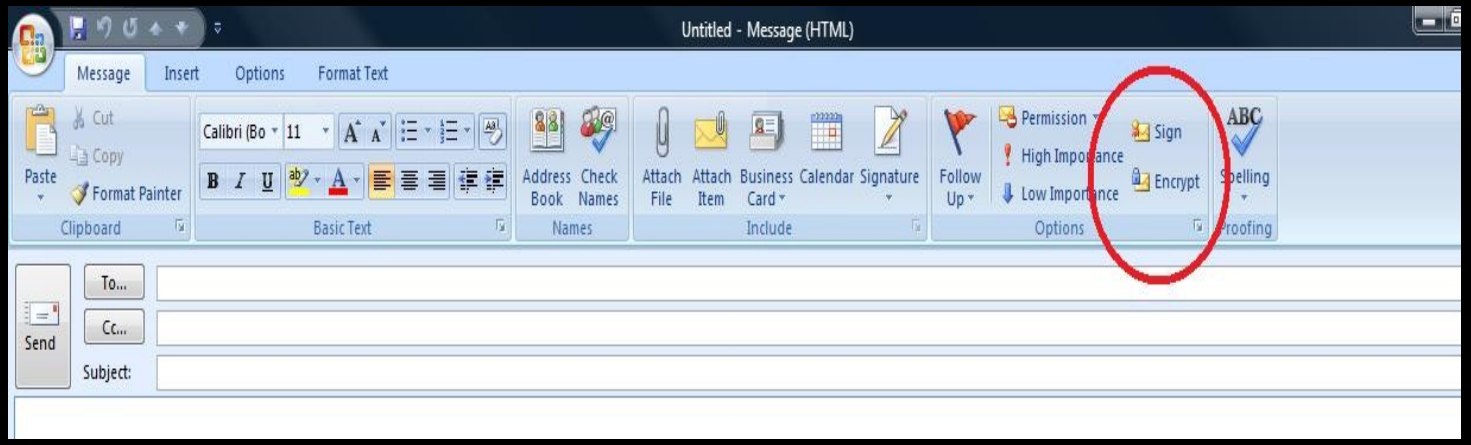
If you aren't comfortable placing the same information on a sign in your front yard, don't put it online.

OPSEC Countermeasures

E-mail can be intercepted and read by an adversary, unless it’s encrypted.

MS Outlook can encrypt e-mail with a digital certificate.

Other encryption is also an option.



OPSEC Countermeasures

Telephones are NOT secure!

Cell phones, cordless phones and land-lines can all be compromised. Limit what you discuss on the phone because you never know who could be listening in on you.

Consider: Digital Enhanced Cordless Telecommunications (DECT) Phones

OPSEC Countermeasures

- Telemarketing calls may be legitimate... or they may be scams. Calls can also be attempts at information collection, or harassment.

- Add your telephone numbers to the ‘National Do Not Call Registry’.

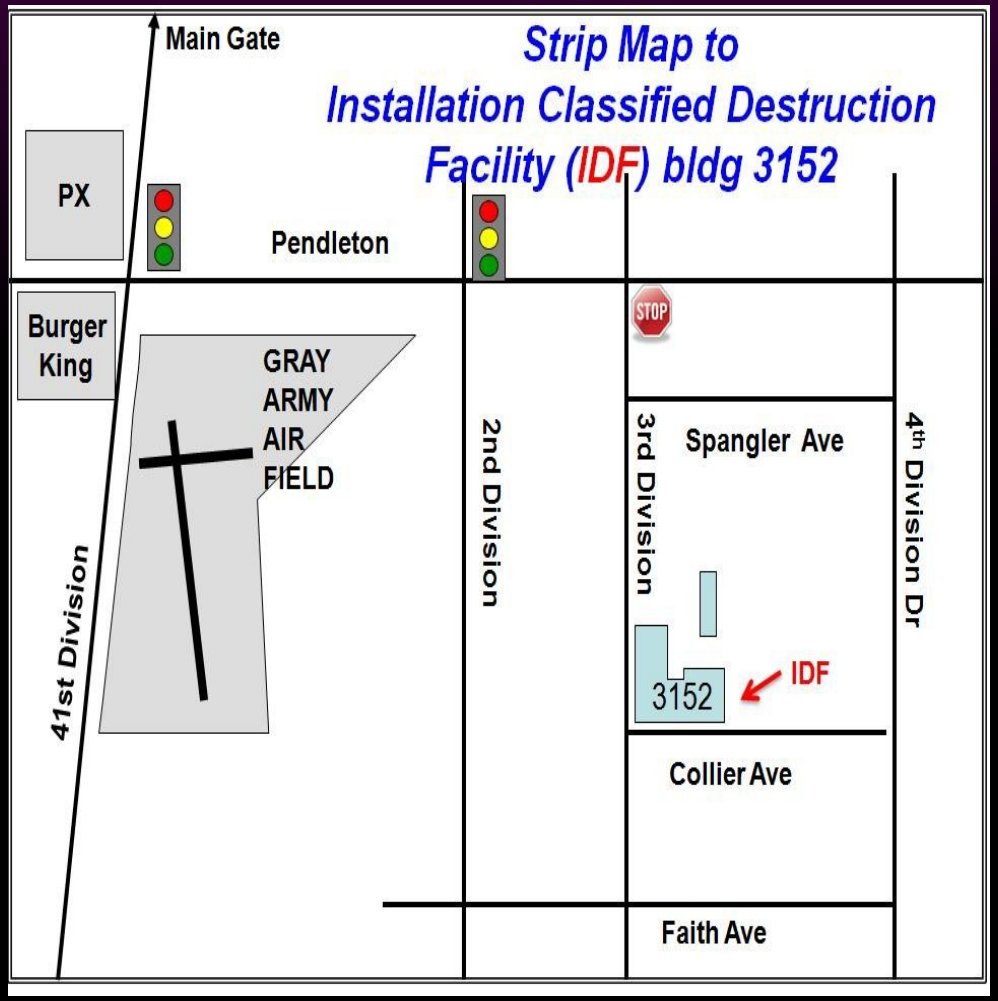
  https://www.donotcall.gov/register/reg.aspx

- OPT OUT of pre-screening of your credit

OPSEC Countermeasures

Personal Shred Day

- Installation Destruction Facility
- Last Friday of the Month 0800-1130
- Building 3152 on the corner of 3rd Division and Collier



OPSEC Countermeasures

- Do not use your military ID for other than military purposes.

- Never allow anyone to make
- copy of your military ID
- – it’s illegal to do so.

OPSEC Countermeasures

Create A PIN Lock For Your Voicemail - No pass code for your voicemail? Then anyone with phone-number "spoofing" software can call your carrier's voicemail number and get right into your account. Enable the pass code, and don't stick with the carrier's default PIN, such as "1234" or "9999" — hacker and creeps already know those.

Turn on encrypted social-media connections - One year ago, it was easy for cyberspies to sit in cafes and snoop on other people's social-networking posts. Today, Facebook, Twitter and Google+ all let you change your settings so that encrypted ("https") connections are always on, locking out the spies.

Put a screen lock on your smartphone - Your smartphone may be valuable, but even more valuable is all the personal information you've got on it. To make sure anyone who finds or steals it can't see your data, enable the screen lock, which asks for a PIN or pattern before the phone can be used. (The phone can still be answered if it rings.)

Enable wireless encryption - Most home wireless routers are set by default to transmit signals unencrypted. But that lets anyone snoop on your Internet traffic. Set your router to encrypt its transmissions, and pick a strong password so that only those machines you permit can access it.

OPSEC Questions

- Questions?

OPSEC Resources

- DES OPSEC Page:
http://www.lewis-mcchord.army.mil/des/le_opsec.htm

- National OPSEC Program
  Interagency OPSEC Support Staff
https://www.iad.gov/ioss/

- Michael Chesbro, DES OPSEC Officer, 253-966-7303

DES OPSEC Bulletin – Via E-mail to You!